

УДК 621.391

О БИНАРНЫХ ПОСЛЕДОВАТЕЛЬНОСТЯХ С ПЕРИОДАМИ $2p$ И $4p$ НА ОСНОВЕ КЛАССОВ БИКВАДРАТИЧНЫХ ВЫЧЕТОВ

И.С.Вагунин, В.А.Едемский

Институт электронных и информационных систем НовГУ, Vladimir.Edemsky@novsu.ru

Рассчитаны параметры ряда бинарных последовательностей с периодами $2p$, $4p$ и близкой к идеальной периодической автокорреляционной или взаимно корреляционной функцией. Последовательности формируются на основе классов биквадратичных вычетов.

Ключевые слова: бинарные последовательности, классы биквадратичных вычетов, корреляционные функции

Parameters of series of binary sequences with the periods $2p$, $4p$ and close-to- perfect autocorrelation or crosscorrelation function are calculated. The sequences are formed on the basis of biquadratic residue classes.

Keywords: binary sequences, biquadratic residue classes, corelation function

1. Введение

Периодические бинарные последовательности (БП) $z_i = \{\pm 1\}$ широко применяются в различных областях, например в системах связи, радиолокации и гидролокации [1,2]. Одной из важных характеристик БП Z является ее периодическая автокорреляционная

функция (ПАКФ) $\lambda_Z(\tau) = \sum_{i=0}^{N-1} z_i z_{i+\tau}$, здесь N — пе-

риод БП. Хорошо известны БП, соответствующие разностным множествам и обладающие одноуровневой ПАКФ [1,2]. Существенный недостаток таких БП заключается в том, что число известных разностных множеств ограничено [2,3]. В [4,5] была предложена методика анализа и синтеза дискретно-кодированных последовательностей, сформированных на основе

классов степенных вычетов по простому модулю, с заданными ограничениями на совокупность характеристик. По этой методике в [6] были синтезированы бинарные последовательности с периодом $2p$ и квазиидеальной (близкой к идеальной) ПАКФ. Цель настоящей статьи заключается в синтезе БП с квазиидеальной ПАКФ, а так же пар БП с квазиидеальной периодической взаимно корреляционной функцией (ПВКФ). Последовательности будут формироваться с использованием классов биквадратичных вычетов по правилу кодирования, отличному от использованного в [6].

Такие последовательности могут быть использованы в радиотехнических системах связи и передачи информации, радионавигации с шумоподобными сигналами, фазовой или амплитудно-фазовой манипуляцией и корреляционной обработкой сигналов.

2. Формирование БП

Рассмотрим БП Z с периодом $2N$, сформированную на основе двух БП $X = \{x_j\}$, $Y = \{y_j\}$ периода N по правилу кодирования (ПК)

$$z_i = \begin{cases} x_j, & \text{если } i = 2j, \\ y_j, & \text{если } i = 2j+1, \end{cases} \quad (1)$$

здесь i, j — целые числа. Согласно [5], для ПАКФ БП Z имеем

$$\lambda_Z(\tau) = \begin{cases} \lambda_X(n) + \lambda_Y(n), & \text{если } \tau = 2n, \\ r_{X,Y}(n) + r_{Y,X}(n+1), & \text{если } \tau = 2n+1, \end{cases} \quad (2)$$

где $\lambda_X(n), \lambda_Y(n), r_{X,Y}(n), r_{Y,X}(n)$ — соответственно ПАКФ и ПВКФ пары БП X, Y . Аналогично, если пара БП Z_1 и Z_2 сформирована по ПК (1) для последовательностей X_1, Y_1 и X_2, Y_2 , то для ПВКФ пары последовательностей справедливо соотношение

$$r_{Z_1, Z_2}(\tau) = \begin{cases} r_{X_1, X_2}(n) + r_{Y_1, Y_2}(n), & \text{если } \tau = 2n, \\ r_{X_1, Y_2}(n) + r_{Y_1, X_2}(n+1), & \text{если } \tau = 2n+1. \end{cases} \quad (3)$$

Таким образом, предложенное ПК формирует БП с периодом $2N$, ПАКФ которых, а также ПВКФ пары БП определяются ПАКФ и ПВКФ БП периода N , что позволяет использовать для синтеза БП результаты, полученные ранее. В частности, результаты анализа и синтеза БП с простым периодом p , сформированных на основе классов биквадратичных вычетов [5].

В следующих разделах рассмотрим задачу синтеза уравновешенных бинарных последовательностей с периодами $2p$ и $4p$ на основе классов биквадратичных вычетов с квазиидеальной ПАКФ, т.е. с $\max_{\tau=1, N-1} |\lambda_Z(\tau)| \leq \lambda_{\max}$, а также пар БП периода $2p$ и

ПВКФ: $\max_{\tau=0, 2p-1} |r_{Z_1, Z_2}(\tau)| \leq r_{\max}$, где $\lambda_{\max}, r_{\max}$ — заданные пороговые числа. Предварительно рассмотрим необходимые условия существования БП с квазиидеальной ПАКФ.

3. Необходимые условия существования БП с квазиидеальной ПАКФ на основе классов биквадратичных вычетов

Пусть $p = 4R + 1$, где R — натуральное число и θ — первообразный корень по модулю p . Обозначим через $H_k = \{\theta^{k+dv}, v = \overline{0, R-1}\}$ — класс степенных вычетов с номером k , $k = \overline{0, 3}$.

Рассмотрим пару БП X, Y , сформированных по обобщенному ПК [1]

$$U_X(j) = \begin{cases} 1, & \text{если } j \in H_m, m \in I_X, \\ -1 & \text{в ост. случаях;} \end{cases} \quad (4)$$

$$U_Y(j) = \begin{cases} 1, & \text{если } j \in H_m, m \in I_Y, j = 0, \\ -1 & \text{в ост. случаях.} \end{cases}$$

Здесь I_X, I_Y — подмножества индексов, $m = \overline{0, 3}$.

ПАКФ и ПВКФ БП X, Y , сформированных по ПК (4), однозначно определяются таблицей спектров

разностей классов биквадратичных вычетов (СРКВ) $S(0, \Delta)$, где $\Delta = \overline{0, 3}$, в частности, значения ПАКФ и ПВКФ БП будут постоянны на классах биквадратичных вычетов [2].

Лемма 1. Если $p > 41$, то для любых $k, l = \overline{0, 3}$ всегда существует $t = \overline{1, p-1}$ такое, что t принадлежит классу биквадратичных вычетов с номером k , а $(t+1)$ — с номером l .

Доказательство. В [5] показано, что для четного R справедливо равенство $16S(0,0) = (p-11-6x, p-3+2x+8y, p-3+2x, p-3+2x-8y)$, а для нечетного R

$16S(0,0) = (p-7+2x, p-3-2x, p-7+2x, p-3-2x)$, где $p = x^2 + 4y^2$, $x \equiv 1 \pmod{4}$, x, y — целые числа.

Таким образом, если $p > 41$, то из представления СРКВ следует, что все гармоники $S(0,0)$, а значит и $S(l,l)$ отличны от нуля. По определению СРКВ $S(l,l)$ существует $q \in H_l$ такое, что $(q-1) \in H_k$, тогда $t = q-1$ [2]. Лемма доказана.

Лемма 2. Если $p > 41$, то для ПАКФ БП Z , сформированной по ПК (1), имеем $\max_{\tau} |\lambda_Z(\tau)| \geq 2 \max_{n \neq 0} |r_{X,Y}(n)|$.

Доказательство. Если $\tau = 2n+1$, то $\lambda_Z(\tau) = r_{X,Y}(n) + r_{Y,X}(n+1)$ по формуле (2), причем ПВКФ $r_{X,Y}(n), r_{Y,X}(n)$ постоянны на классах биквадратичных вычетов [2]. Таким образом, если $\max_{n \neq 0} |r_{X,Y}(n)|$ достигается на k -м классе, а $\max_{n \neq 0} |r_{Y,X}(n)|$ — на l -м классе, то по лемме 1 для $p > 41$ найдется n такое, что $r_{X,Y}(n) = r_{Y,X}(n+1)$. Тогда $\lambda_Z(\tau) = 2r_{X,Y}(n)$, что и доказывает лемму 2.

Согласно лемме 2, если $\max_{\tau=1, 2p-1} |\lambda_Z(\tau)| \leq \lambda_{\max}$, то $\max_{\tau=1, p-1} |r_{X,Y}(n)| \leq \lambda_{\max} / 2$.

Таким образом, если БП Z , сформированная по ПК (1), обладает квазиидеальной ПАКФ, то пара БП X, Y обладает квазиидеальной ПВКФ. Более того, так как $\lambda_Z(1) = r_{X,Y}(0) + r_{Y,X}(1)$, то и значение $r_{X,Y}(0)$ должно быть мало. ПВКФ пар БП, сформированных по правилу (4), были вычислены в [5]. Согласно полученным результатам регулярное ПК пар БП на основе классов биквадратичных вычетов с малыми значениями ПВКФ для $\tau = \overline{0, p-1}$, существует, с точностью до циклического сдвига и перестановки, в единственном варианте, когда $I_X = \{0,1\}$, $I_Y = \{1,2\}$. Исследуем БП для таких I_X, I_Y в следующем разделе.

4. Синтез уравновешенных БП с периодом $2p$ и квазиидеальной ПАКФ или ПВКФ

Если $I_X = \{0,1\}$, то справедливы следующие взаимно однозначные соответствия [5]:

для четного R

$$\lambda_X(n) \Leftrightarrow (-3+2y, -3-2y, 1+2y, 1-2y), \quad (5)$$

для нечетного R

$$\lambda_X(n) \Leftrightarrow (-1-2y, -1+2y, -1-2y, -1+2y), \quad (6)$$

(знак $\Leftrightarrow$ означает, что если $\langle \tau \rangle_p \in H_f$, то $\lambda_X(\tau)$ совпадает с f -й гармоникой СРКВ [2]).

ПВКФ пары БП X, Y была найдена в [5] при $y_0 = -1$. Учитывая, что изменение знака y_0 равносильно добавлению $\Delta(0) = 2x_{p-\tau}$ к значениям ПВКФ $r_{X,Y}(n)$ и $\Delta(0) = 2x_\tau$ к значениям ПВКФ $r_{Y,X}(n)$, получаем из [5] следующие соответствия:

для четного R

$$r_{X,Y}(n) \Leftrightarrow (2+x, -x, x-2, -x), \quad r_{X,Y}(0) = -1, \quad (7)$$

для нечетного R

$$r_{X,Y}(n) \Leftrightarrow (-x, -2+x, -x, 2+x), \quad r_{X,Y}(0) = -1. \quad (8)$$

Теорема 1. Если БП X, Y сконструированы по ПК (4) при $I_X = \{0,1\}$, $I_Y = \{1,2\}$, то для ПАКФ БП Z , сформированной по ПК (1), $\max |\lambda_Z(\tau)| \leq 4+2|x|$, $\tau = \overline{1, 2p-1}$.

Доказательство. Если $\tau = 2n$, то по формуле (2) справедливо равенство $\lambda_Z(\tau) = \lambda_X(n) + \lambda_Y(n)$. Из свойств СРКВ следует, что формулы (5) и (6) будут справедливы для ПАКФ БП Y при циклическом сдвиге в правой части элементов матрицы на единицу. После суммирования получаем, что $\lambda_Z(\tau) = -2$, $\tau \neq 0$, если R нечетное, и $\lambda_Z(\tau) = \pm 2, -6$, $\tau \neq 0$, если R четное.

Если же $\tau = 2n+1$, то по (2) имеем $\lambda_Z(\tau) = r_{X,Y}(n) + r_{Y,X}(n+1)$, тогда из формул (7) и (8) следует, что значения ПАКФ $\lambda_Z(\tau) \in \{1+x, \pm 2, \pm 2x, -2x \pm 4\}$ для четного R и $\lambda_Z(\tau) \in \{-1-x, \pm 2, \pm 2x, -2x \pm 4\}$ для нечетного R , $\tau = \overline{1, 2p-1}$. Таким образом, $\max_{\tau=\overline{1, 2p-1}} |\lambda_Z(\tau)| \leq 4+2|x|$, и теорема доказана.

Согласно лемме 2, если $p > 41$, то $\max_{\tau=\overline{1, 2p-1}} |\lambda_Z(\tau)| = 4+2|x|$. Таким образом, при $p > 41$ наименьшее возможное значение бокового лепестка ПАКФ БП в условиях теоремы 1 равно шести, т. е. рельеф ПАКФ при $p = 1+4y^2$ несколько отличается от оптимального при $N \equiv 2 \pmod{4}$ ($\lambda_Z(\tau) = \{\pm 2\}$, $\tau = \overline{1, 2p-1}$) [1], но несущественно.

Теорема 1 задает достаточные условия синтеза уравновешенных БП с ПАКФ, близкой к оптимальной, БП Z будет удовлетворять заданным ограничениям при $p = x^2 + 4y^2$, $4+2|x| \leq \lambda_{\max}$.

Аналогично можно сконструировать и пары БП с квазиидеальной ПВКФ, о чем свидетельствует следующая теорема.

Теорема 2. Если пары БП X_1, Y_1 и X_2, Y_2 определены ПК (2) при $I_{X_1} = \{0,1\}$, $I_{Y_1} = \{2,3\}$ и

$I_{X_2} = \{1,2\}$, $I_{Y_2} = \{0,3\}$, то для ПВКФ пары БП Z_1, Z_2 , сформированных по ПК (1), $\max |r_{Z_1, Z_2}(\tau)| \leq 4+2|x|$, $\tau = \overline{0, 2p-1}$.

Доказательство. Согласно формуле (3) ПВКФ пары БП Z_1, Z_2 определяется ПВКФ $r_{X_1, X_2}(n), r_{Y_1, Y_2}(n), r_{X_1, Y_2}(n), r_{Y_1, X_2}(n+1)$, значения которых при $n \neq 0$ ($n+1 \neq p$) определены формулами (7,8), а при $n = 0$ равны ± 1 . Рассматривая все возможные комбинации слагаемых, после суммирования получаем, что заведомо $r_{Z_1, Z_2}(\tau) \in \{\pm 2, \pm(x+1), \pm(x-3), \pm 2x, \pm 2x \pm 4\}$ при $\tau = \overline{0, 2p-1}$. Из последнего соотношения и следует утверждение теоремы 2.

Теорема 2 определяет достаточные условия существования пар БП с квазиидеальной ПВКФ. Если $4+2|x| \leq r_{\max}$, то пара уравновешенных БП с периодом $2p$, $p = x^2 + 4y^2$ удовлетворяет заданному ограничению.

5. Синтез БП с периодом $4p$ и квазиидеальной ПАКФ

Рассмотрим еще один пример синтеза БП с квазиидеальной ПАКФ, также с использованием классов биквадратичных вычетов. В [7] исследованы ПАКФ БП, сформированных по ПК

$$U_X(j) = \begin{cases} 1, & \text{если } j \in (H_{0,0} \cup H_{0,1} \cup H_{1,0} \cup H_{1,3}), \\ -1 & \text{в ост. случаях,} \end{cases} \quad (9)$$

где $H_{j,k} = \{a \mid a = \overline{1, 2p-1}, \langle a \rangle_2 = j, \langle a \rangle_p \in H_k\}$, $\langle a \rangle_p$ — наименьший положительный вычет натурального числа a по модулю p , $j = 0,1, k = \overline{0,3}$, при этом $H_{j,k} \cong \{j\} \times H_k$.

Рассмотрим еще одну БП Y , сформированную по ПК, аналогичному правилу (9):

$$U_Y(j) = \begin{cases} 1, & \text{если } j \in (H_{0,1} \cup H_{0,2} \cup H_{1,0} \cup H_{1,1}), \\ -1 & \text{в ост. случаях,} \end{cases} \quad (10)$$

и исследуем ПВКФ пары БП X, Y .

Лемма 3. Если пара БП X, Y формируется по ПК (9,10), то рельеф ее ПВКФ равен $r_{X,Y}(n) = \{\pm 2, \pm 2 \pm 4y\}$, $\tau = \overline{0, 2p-1}$.

Доказательство. В [5] показано, что ПВКФ пары БП X, Y равна

$$r_{X,Y}(\tau) = \begin{cases} r_{X_1, Y_1}(\langle \tau \rangle_p) + r_{X_2, Y_2}(\langle \tau \rangle_p), & \text{если } \tau = 2n, \\ r_{X_1, Y_2}(\langle \tau \rangle_p) + r_{X_2, Y_1}(\langle \tau \rangle_p), & \text{если } \tau = 2n+1. \end{cases}$$

Здесь $I_{X_1} = \{0,1\}$, $I_{X_2} = \{0,3\}$ и $I_{Y_1} = \{1,2\}$, $I_{Y_2} = \{0,1\}$.

Таким образом, $r_{X,Y}(0) = 2$, а при $\tau \neq 0$ ПВКФ $r_{X_1, X_2}(\langle \tau \rangle_p)$ определена формулами (7), (8), которые при циклическом сдвиге в правой части элементов матрицы на единицу будут справедливы и для ПВКФ $r_{X_2, Y_2}(\langle \tau \rangle_p)$. После суммирования получаем, что $r_{X,Y}(\tau) = \pm 2$, $\tau = 2n$.

ПВКФ пары последовательностей X_1, Y_2 совпадает с ПАКФ БП, сформированной по ПК (4) при $I_X = \{0,1\}$ и задается формулами (5,6). Согласно [5] для ПВКФ пары БП X_2, Y_1 будут справедливы следующие взаимно однозначные соответствия:

для четного R

$$\lambda_X(\langle \tau \rangle_p) \Leftrightarrow (1+2y, -1-2y, 1+2y, 1-2y), \quad (11)$$

для нечетного R

$$\lambda_X(\langle \tau \rangle_p) \Leftrightarrow (3-2y, -1+2y, -1-2y, 3+2y). \quad (12)$$

После суммирования по формулам (5,6,11,12) получаем, что $r_{X,Y}(\tau) = \pm 2 \pm 4y$, $\tau = 2n+1$, $\tau \neq p$; $r_{X,Y}(p) = 2$. Лемма доказана.

Теорема 3. Если пара БП X, Y сконструирована по ПК (9,10), то для ПАКФ БП Z сформированной по ПК (1), $\max|\lambda_Z(\tau)| \leq 4+8|y|$, $\tau = 1, 4p-1$.

Доказательство. Автокорреляционные функции двоичных последовательностей, соответствующих рассматриваемым БП, были рассчитаны в [5,7,8]. Откуда и следует, что при нечетном R ПАКФ $\lambda_X(\tau) \Leftrightarrow (2x, -2x, 2x, -2x)$, если $\tau = 2n+1$, $\tau \neq p$, $\lambda_X(\tau) = -2$ при $\tau = 2n$ и $\lambda_X(p) = 2$, а при четном R $\lambda_Y(\tau) \Leftrightarrow (-2x, 2x, -2x, 2x)$, $\tau = 2n+1$, $\tau \neq p$; $\lambda_Y(\tau) \Leftrightarrow (-6, -2, 2, -2)$, $\tau = 2n$; $\lambda_Y(p) = 2$. Суммируя по формуле (2), получаем, что $\lambda_Z(\tau) = \{0, \pm 4\}$, $\tau = 2n$, если R нечетное, и $\lambda_Z(\tau) = \{-8, 0, 4\}$, $\tau = 2n$, если R четное. Если же $\tau = 2n+1$, то из (3) и леммы 3 следует, что $\max|\lambda_Z(\tau)| \leq 4+8|y|$, что и доказывает теорему 3.

Теорема 3 определяет достаточные условия синтеза БП с периодом $4p$ и квазиидеальной ПАКФ,

БП будет удовлетворять заданным ограничениям при $p = x^2 + 4y^2$, $4+8|y| \leq \lambda_{\max}$.

6. Заключение

Синтезирован ряд новых уравновешенных бинарных последовательностей с периодом $2p$ и автокорреляционной или взаимно корреляционной функцией, близкой к идеальной. Определены параметры бинарных последовательностей с периодом $4p$ и квазиидеальной автокорреляционной функцией. Последовательности формируются на основе классов биквадратичных вычетов.

1. Свердлик М.Б. Оптимальные дискретные сигналы. М., 1975. 200 с.
2. Гантмахер В.Е., Быстров Н.Е., Чеботарев Д.В. Шумоподобные сигналы. Анализ, синтез, обработка. СПб.: Наука и техника, 2005. 400 с.
3. Холл М. Комбинаторика. М.: Мир, 1970. 423 с.
4. Gantmakher V.E., Edemskiy V.A. The Synthesis Methodology of Periodic Discretely Coded Sequences Formed Basing on Cyclotomic Classes with Basic Parameters Constraints // Proceedings of 2007 International Workshop on Signal Design and Its Applications in Communications (IWSDA'07). China, 2007. P.4-8.
5. Едемский В.А., Гантмахер В.Е. Синтез двоичных и троичных последовательностей с заданными ограничениями на их характеристики. В.Новгород.: НовГУ, 2009. 189 с.
6. Едемский В.А., Вагунин И.С. // Физика и механика материалов: Приложение к Вестнику НовГУ. 2009. №50. С.26-29.
7. Ding C., Helleseht T., Martinsen H. // IEEE Trans. Info. Theory. Jan 2001. Vol. IT-47. P.428-433.
8. Едемский В.А., Вагунин И.С. // Журнал научных публикаций аспирантов и докторантов. 2008. № 6. С.147-150.